Application No:	GB 0216690.8	**Examiner:**	Joseph Wellings
Claims searched:	All	**Date of search:**	21 January 2003

Patents Act 1977 : Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance	
X	1, 5-7, 10-13	EP 1050992 A1	See for example English language translations of abstract and paragraphs [0011] to [0013].
X	1, 5-7, 10-13	EP 0673154 A1	(PUMPKIN HOUSE) See particularly column 1, line 50 to column 3, line 44.
X	1, 5-7, 10-13	EP 0343805 A2	(GENERAL INSTRUMENT) See for example column 2, line 41 to column 3, line 52; and column 6, line 57 to 8, line 17.
A		US 4688250 A	(CORRINGTON)

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[V]:

H4P

Worldwide search of patent documents classified in the following areas of the IPC[7]:

H04L

The following online and other databases have been used in the preparation of this search report:

WPI, EPODOC, PAJ

EPODOC / EPO

PN - EP1050992 A 20001108

PD - 2000-11-08

PR - EP19990108960 19990506

OPD - 1999-05-06

TI - Data encryption method

AB - The data protection method has an initial data set transferred between 2 parties, with the receiving party transferring the to a third party at which it is associated with a private code, used for generating a key employed for encoding subsequent data supplied from the first party. The data received by the second party is transferred to the third party for decoding, with subseq transmission of the decoded data back to the second party.

IN - JACOB HANSJOERG K (CH)

PA - ITC & C SUSANNE JACOB (CH)

EC - H04L9/30 ; G07F19/00F6

IC - H04L9/30 ; G07F7/10

CT - EP0797329 A [A]; XP000742245 A [A]

CTNP - [A] MAMBO M ET AL: "PROXY CRYPTOSYSTEMS: DELEGATION OF THE POWER TO DECRYPT CIPHERTEXTS" IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, Bd. E 80-A, Nr. 1, 1. Januar 1997 (1997-01-01), Seiten 54-63, XP000742245 ISSN: 0916-8508

© WPI / DERWENT

TI - Data encoding method e.g. for e-business, has data transmitted between 2 parties encoded via key generated using private code known only to third party

PR - EP19990108960 19990506

PN - EP1050992 A1 20001108 DW200102 H04L9/30 Ger 009pp

PA - (ITCC-N) ITC & C JACOB SUSANNE

IC - G07F7/10 ;H04L9/30

IN - JACOB H K

AB - EP1050992 NOVELTY - The data protection method has an initial data set transferred between 2 parties, with the receiving party transferring the data to a third party at which it is associated with a private code, used for generating a key employed for encoding subsequent data supplied from the first party. The data received by the second party is transferred to the third party for decoding, with subsequent transmission of the decoded data back to the second party.

- USE - The method is used for protecting data transmitted electronically, e.g. for e-business.
- ADVANTAGE - The method protects the encryption code for the electronically transmitted data.
- DESCRIPTION OF DRAWING(S) - The figure shows a schematic representation of a connection between an e-business customer and a secure service.
- (Dwg. 1/2)

OPD - 1999-05-06

DS - AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

AN - 2001-009675 [02]

[0001] the invention refers to a procedure for the encoding of data.
[0002] it is well-known that so-called enamels, on electronic way sent away messages, offer hardly to protection against eavesdroppers. One tries to encode therefore the message, so that only the legal recipient can read contents. More rapid and cheaper computers as well as high performance algorithms made suitable systems generally accessible for the eighties.
[the US secret service, national the Security Agency (NSA) possessed 0003] to for instance in the middle of the seventies, practically a monopole at the American encoding technology. That changed 1976, as Whitfield Diffie and Martin E. Hellman of the University of Stanford (California) for the first time the procedure of publication IC key cryptography published (in German one speaks by Kryptosystemen with published code or by asymmetrical code-systems). Up to this publication only one key to the en and decoding messages served. Such systems symmetrically specified can function only if the code will transfer over a safe channel, what the procedure become often unmanageable let. If one can transfer it however surely, why then not equal the message itself?
[0004] publication IC key cryptography operates asymmetrically, without requiring transferring codes. Are needed instead of its two different, but to each other complementary codes. Each code does not decipher the message, which coded that different complementary codes in each case, can however its own factory itself again reconvert. Therefore the owner may make one of it public without doubts (public keys), while it must keep the other one secret (private keys).
[0005] asymmetrical cryptography uses the fact that some mathematical functions in a direction can be calculated quite easily, while its reversal is unsolvable. The two general agents are developed the Diffie Hellmann algorithm with its versions and the RSA Chiffriersystem, at the Massachusetts Institute of Technology in Cambridge. The first method uses that the calculation of discrete logarithms is heavy. The RSA Chiffriersystem is based on the difficulty of the prime number dismantling. It is easy to multiply two large prime numbers together but very with difficulty to divide the product again in its factors.
[0006] a further application of asymmetrical cryptography is the proof of the authenticity of the messages. If B transmits a message to A, it encodes it first with its personal and afterwards again with A's open code. A proceeds in reverse: It entschlueselt the message first with its personal code and then again with B's open code. If the decoded text is readable, it must come from B.
[ ] nevertheless unfortunately the cryptology with public codes of two disadvantages has 0007: It is time-consuming for longer messages and the coding process leaves sometimes regularities in the text unchanged, which makes to crack the code more easily.
[0008] however does not offer also these coding methods absolute protection against a decoding. Thus a particularly designed parallel computer of the electronics Foundation in San Francisco decoded a DES message, by trying all conceivable 56-Bit-Schluessel one after the other within one week. Also the publication IC key system can be tested, approximately by coding special texts with the open code and analysis of the results.
[0009 beyond that] needs everyone took part a private code, which it must keep secret, what with an appropriate noticing expenditure is connected.
[0010] the invention is the basis the problem to place a coding procedure for the order the fact that a higher security offers as well as reduces the expenditure for the coding for the involved ones.
[0011] the invention solve this function by the engagement of a third party C, which assigns

or also directly to the party C reset data a private code to the data transmitted by the party A to the party B, from which again a complementary public code is calculated. The public code is set for example by data network of the party A, which codes thereby now its to the party B or to the party C reset messages. The party B cannot decode however the message, since it does not have an access to the private code. The party B transmits now the coded message to the third party C, which the message coded with the public code again decoded and which sends message back decoded now to the party B. By the third party C the party B is not loaded by en and decoding processes and it can be nevertheless safe that it actually communicates with the correct party A or transacts business, since only the data outgoing from this party A can be decoded.

[0012] for sales on electronic way as for example over the Internet this type of the encoding is suitable in particular, in order to manufacture the necessary confidence between the buyer and the salesman. So it can be guaranteed for example that the salesman has to actually do it with the person or institution, who outputs themselves as a party A. In order at expense of the party A of business to transact, is prevented an abuse by third, which outputs itself as a party A, thereby. So for example the party A can indicate their name and its credit card number for the first internal message. In order to increase security, this first internal message cannot be handled over the party B, but the party A approaches directly with the party C, which assigns a private code, which generates again a public code to the credit card number in connection with the name of A. The public code is set for the party A, which encodes thereby zukuenfig its credit card number, so that the encoded credit card number is only sent away over the network. The party B, which receives this encoded credit card number, decodes it however now not, but passes it on to the party C. The party C knows the private key to the decoding of the encoded credit card number and transmits to the decoding the decoded number to the party B, which can be safe now to do it with the person A to actually have, since only this is provided with the public code, which corresponds to the private code.

[0013] by security to increase, however additionally a new private code can be assigned, then a public code generated after each transaction to the party A by the party C. Even if a ungebetener eavesdropper the public code guess, then it this does not use anything for the following transaction, since another public code for sending the message away is then already used.

[ ] a decoding of messages is possible for 0014 only by manipulations of the party C, so that it must be guaranteed that it concerns an absolutely trustworthy institution here. This is however a political and no technical question.

[0015] further details and advantages of the invention result from the following description and the drawing. In the drawing the figures 1 and 2 show a schematic representation of an execution example of the invention on the basis of transactions between customers and suppliers:

Fig.1: schematic representation of the connection between a customer and a code service;
Fig.2: schematic representation of the connection between a customer and a supplier.

[0016] the execution example represented schematically in the Fig. 1 and 2 illustrates, how the invention can be used in particular for sales on electronic way as for example over the Internet, in order to guarantee the necessary confidence between the buyer and the salesman. At the beginning of a transaction between customers and suppliers, a potential customer K1 (a party A) turns appropriately to a code service SD (a party C) and logs on there with its name. It is favourable-proves beyond that possible that the potential suppliers (a party B) are

attainable over the code service only, so that a direct establishment of contact between the customers K and the supplier L is not possible. So that the customer K1 experiences, with which suppliers L he can step over the code service SD into contact, is it in particular appropriate that the customer K1 can inform first completely witthout obligation without denomination of his name about the supply of the code service SD. However it is also conceivable in the context of the invention that the customer K1 comes closer first at the supplier L1 and this refers it to the code service SD and it described that only including the code service SD it is possible, with it, the supplier L1, a business to transact.
[the code service SD in its internal data base looks 0017 up] after the message of the name of K1 whether this name already admits to it is. If this is not the case, then the code service creates SD favourable-proves first an identification code IC, which it sets for the K1 appropriately not on electronic way, but by post office, and enters beyond that K1 with the identification code into its data base. In particular it can be intended that before the entry of the K1 into the customer file the code service can be acknowledged again from K1 that the entry is actually required, in order to make no unnecessary entries.
[ ] the identification code IC K1 uses 0018 now with the next transaction with the code service, by sending SD the identification code unverschuesselt. Appropriately effected only after this second transaction the final entry of the customer K1 into the customer data bank from SD. via the additional use of an identification code, which is used only once for the final entry of the K1 into the customer file and is not elekronisch set, increases security, since K1 does not step now with its direct name etc. in connection with the code service SD, but already under a code name.
[0019] the code service SD creates now for K1 a private code and calculates from it a public code, which the code service SD sets for the K1 on electronic way. In order to increase security, however favourable-proves with each transaction of the K1 with the code service SD or a supplier L1 the code service SD knows a new private code and then from it a new public code for the customer K1 to generate. Even if a ungebetener eavesdropper the public code guess, then it this does not use anything for the following transaction, since another public code is then already used.
[the customer K1 for example also its credit card number, his personal finger mark or the sample of its iris with the public code can encode 0020] apart from its name and his address and send over the network to the code service SD, which decodes the data with the private code and stores these data in the data base.
[0021] after now the code service all important data of the customer K1, which is necessary in particular for the business between the customer, which can be transacted, K1 and one or more suppliers a L1-Ln, the code service SD the customer K1 the receipt to all suppliers gespeichet, opens, with whom the code service co-operates.
[with the fact 0022] it is conceivable that all business is handled only over the code service SD, so that the customer K1 its desire, with which supplier L1 it wants to co-operate, to which SD indicates encoded, which decodes it and thereupon makes the connection between the K1 and a supplier L1.
[ ] the same encoding technique, which was used for the customers, can apply to 0023 thereby also to the suppliers, whereby also more privately in each case and a public code is assigned to the L1. The private code is stored also here with the code service SD, while the public code is set for the L1.
[0024] it is however also possible that the business is handled directly between K1 and L1, whereby L1 makes sure with each transaction with the code service whether it actually concerns the customer K1, when that outputs itself the institute for person communicated

with L1. Only if the true identity of the customer K1 is clarified, the planned business can be handled. In order at expense of the K1 of business to transact, is prevented an abuse by third, which outputs itself as a customer K1, thereby. So for example the customer K1 can indicate its name and his credit card number for the first internal message. In order to increase security, like already executed this first internal message is not appropriately handled over the supplier L1, but the customer K1 approaches directly with the code service SD, which the credit card number in connection with the name of A a private code assigns, which generates again a public code. The public code is set for the customer K1, which encodes thereby zukuenfig the credit card number, so that the encoded credit card number is only sent away over the network. The supplier L1, which receives this encoded credit card number, decodes it however now not, but passes her on to the code service SD. SD knows the private key to the decoding of the encoded credit card number and transmits to the decoding the decoded number at the supplier L1, which can be safe now to do it with the customer K1 to actually have, since only this is provided with the public code, which corresponds to the private code.
[ ] a decoding of messages is possible for 0025 only by manipulations of the code service SD, so that it must be guaranteed that it concerns an absolutely trustworthy institution here. This is however a political and no technical question.
[0026 safer] the invention enables thus by the inclusion of a third party the transmittal of data to arrange and in particular the security of electronically handled sales transactions to increase.

1. Procedure for the coding of data D and information, which are transmitted on electronic way over data transfer us means by a party A to a party B, by the fact characterized that the party A transmits a record D to the party B and/or to a party C first unencrypted and/or provided with a code, whereby the party B passes the data on D to the third party C is generated, and the party C a private code X assigns, which admits only of the party C is to the data D, and from this private code X over an algorithm a public code Y biunique in a direction, set for that the party A and during the following transmittal A to the party B and/or to the party C for the encoding of the data D is used, whereby the party B sends again the encoded data Y(D) to the party C, and decodes the party C with the help of the data Y(D) assigned private code X the data Y(D) and transmits the decoded data D to the party B.
2. Procedure according to demand 2, by the fact characterized that it itself at the party A around a customer, with which a party B concerns around a supplier and at the party C around a code service or such a thing, which is operated by an institution or an organization.
3. Procedure according to demand 1 or 2, by the fact characterized that it concerns with the data D the party A characterizing feature.
4. Procedure according to demand 3, by the fact characterized that it concerns with the data D the name and/or the address of the party A.
5. Procedure according to demand 3, by the fact characterized that it concerns with the data D a general password, a finger mark or the figure of the iris of the eye, which can be assigned to the party A.
6. After procedure or several of the demands 1 to 5, by the fact characterized that after each transmittal of the data Y(D) private codes X assigned by the party A to the party B and/or to the party C that is modified to the data Y(D) by the party C, an accordingly new public code Y2 is generated and these the party A for the next transmittal of the data D is indicated, so that during the next transmittal the data D with the new public code Y2 are encoded and as data Y2(D) are sent away, of the party C with the private code X2 are decoded and then the

decoded data D to the party B are set.

7. After procedure or several of the demands 1, by the fact characterized that during the transmittal provided by data D of the party B to the party A also the party B transmits the data D first unencrypted and/or with a code to the party A and/or to the party C, whereby the party A passes the data on D to the third party C, and the party C a private code X assigns, which admits only of the party C is to the data D, and from this private code X over an algorithm biunique in a direction a public code Y generated, that the party B sets becomes and during the following transmittal of data to the party A and/or to the party C for the encoding of the data D is used, whereby the party A sends now the encoded data Y(D) again to the party C, and decodes the party C with the help of the data Y(D) assigned private code X the data Y(D) and transmits the decoded data D to the party A.

8. After procedure or several of the demands 1-7, by it indicated that after the first establishment of contact of the party A with the party B and/or with the party C a first coding of the party C is sent to the party A on non-electronic way, and that the party A the coding with its second establishment of contact by the party B and/or by the party C it uses.

9. After procedure or several of the demands 1-8, by the fact characterized that the party A and/or the party B and/or the party C can be several persons, institutions or organizations.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 050 992 A1

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
08.11.2000 Patentblatt 2000/45

(51) Int Cl.[7]: **H04L 9/30**, G07F 7/10

(21) Anmeldenummer: **99108960.8**

(22) Anmeldetag: **06.05.1999**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(71) Anmelder: **ITC&C Susanne Jacob**
4056 Basel (CH)

(72) Erfinder: **Jacob, Hansjörg K.**
4056 Basel (CH)

(54) Verfahren zur Verschlüsselung von Daten

(57) Die Erfindung bezieht sich auf ein Verfahren zur Verschlüsselung von Daten und befasst sich mit dem Problem, ein Codierungsverfahren zur Verfügung zu stellen, das eine höhere Sicherheit bietet, sowie den Aufwand für die Codierung für die Beteiligten verringert. Die Erfindung löst diese Aufgabe durch die Einschaltung einer dritten Partei C, die den von der Partei A an die Partei B übermittelten Daten oder auch direkt an die Partei C gerichteten Daten einen privaten Schlüssel zuordnet, aus dem wiederum ein komplementärer öffentlicher Schlüssel berechnet wird. Der öffentliche Schlüssel wird beispielsweise per Datennetz der Partei A zugestellt, die damit nun ihre an die Partei B oder an die Partei C gerichteten Botschaften codiert. Die Partei B selbst kann jedoch die Botschaft nicht decodieren, da sie keinen Zugriff auf den privaten Schlüssel hat. Die Partei B sendet nun die codierte Botschaft an die dritte Partei C, die die mit dem öffentlichen Schlüssel codierte Botschaft wieder entschlüsselt und die nunmehr entschlüsselte Botschaft an die Partei B zurücksendet. Durch die dritte Partei C ist die Partei B durch Ver- und Entschlüsselungsprozesse nicht belastet und sie kann doch sicher sein, dass sie tatsächlich mit der richtigen Partei A kommuniziert oder Geschäfte tätigt, da nur die von dieser Partei A ausgehenden Daten entschlüsselt werden können.

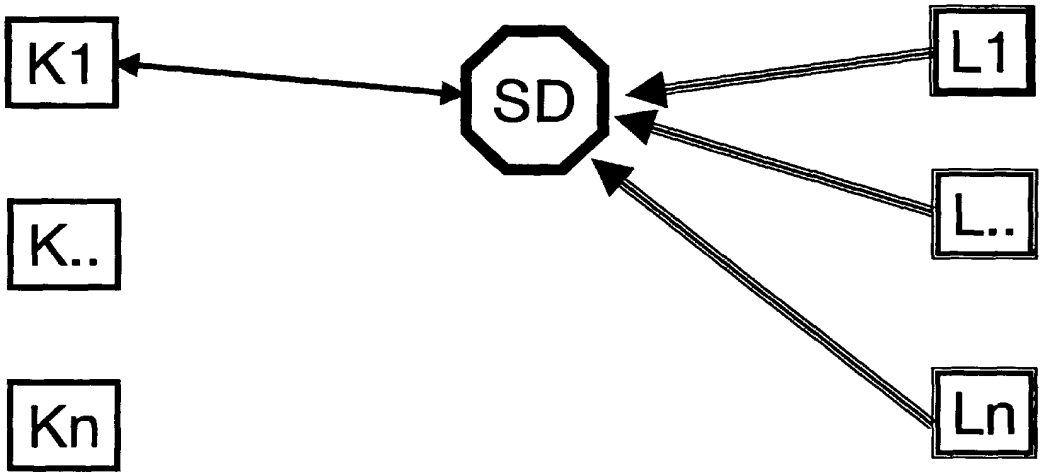

Fig. 1 **ITC&C-1-Pat**

EP 1 050 992 A1

Beschreibung

[0001] Die Erfindung bezieht sich auf ein Verfahren zur Verschlüsselung von Daten.

[0002] Es ist bekannt, dass sogenannte e-Mails, auf elektronischem Weg verschickte Botschaften, kaum Schutz gegen Lauscher bieten. Man versucht daher die Botschaft zu verschlüsseln, so dass nur der rechtmässige Empfänger den Inhalt lesen kann. Schnellere und billigere Computer sowie leistungsstarke Algorithmen haben seit den achtziger Jahren geeignete Systeme allgemein zugänglich gemacht.

[0003] Bis etwa Mitte der siebziger Jahre besass der US-Geheimdienst, die National Security Agency (NSA), praktisch ein Monopol an der amerikanischen Verschlüsselungstechnologie. Das änderte sich 1976, als Whitfield Diffie und Martin E. Hellman von der Universität Stanford (Kalifornien) zum ersten Mal das Verfahren der Public-Key-Kryptographie publizierten (im Deutschen spricht man von Kryptosystemen mit veröffentlichtem Schlüssel beziehungsweise von asymmetrischen Schlüsselsystemen). Bis zu dieser Veröffentlichung diente ein einziger Schlüssel zum Ver- und Entschlüsseln von Nachrichten. Solche symmetrisch genannten Systeme können nur funktionieren, wenn der Schlüssel über einen sicheren Kanal übertragen wird, was das Verfahren oft unhandlich werden lässt. Wenn man ihn jedoch sicher übertragen kann, wieso dann nicht gleich die Nachricht selbst?

[0004] Public-Key-Kryptographie arbeitet asymmetrisch, ohne das Transferieren von Schlüsseln zu erfordern. Benötigt werden statt dessen zwei verschiedene, aber zueinander komplementäre Schlüssel. Jeder Schlüssel entziffert die Nachricht, die der jeweils andere komplementäre Schlüssel codiert hat, kann aber sein eigenes Werk nicht selbst wieder rückverwandeln. Demnach darf der Besitzer einen davon ohne Bedenken publik machen (public key), während er den anderen geheimhalten muss (private key).

[0005] Asymmetrische Kryptographie nutzt die Tatsache, dass sich manche mathematische Funktionen in einer Richtung recht einfach berechnen lassen, während ihre Umkehrung unlösbar ist. Die zwei Hauptvertreter sind der Diffie-Hellmann-Algorithmus mit seinen Varianten und das RSA-Chiffriersystem, entwickelt am Massachusetts Institute of Technology in Cambridge. Die erste Methode nutzt, dass die Berechnung diskreter Logarithmen schwer ist. Das RSA-Chiffriersystem beruht auf der Schwierigkeit der Primzahlzerlegung. Es ist einfach, zwei grosse Primzahlen miteinander zu multiplizieren, aber sehr schwierig, das Produkt wieder in seine Faktoren zu zerlegen.

[0006] Eine weitere Anwendung asymmetrischer Kryptographie ist der Nachweis der Echtheit der Nachrichten. Wenn der B dem A eine Nachricht sendet, verschlüsselt er sie zuerst mit seinem persönlichen und danach noch einmal mit A's offenem Schlüssel. Der A verfährt umgekehrt: Er entschlüselt die Nachricht zuerst mit seinem persönlichen Schlüssel und dann noch einmal mit B's offenem Schlüssel. Wenn der dechiffrierte Text lesbar ist, muss er von B stammen.

[0007] Doch leider hat die Kryptologie mit öffentlichen Schlüsseln zwei Nachteile: Sie ist zeitaufwendig für längere Botschaften und der Chiffrierprozess lässt manchmal Regelmässigkeiten im Text unverändert, was den Code leichter zu knacken macht.

[0008] Allerdings bieten auch diese Codierungsmethoden keinen absoluten Schutz gegen eine Dechiffrierung. So dechiffrierte ein speziell konstruierter Parallelrechner der Electronic Foundation in San Francisco eine DES-Botschaft, indem er innerhalb einer Woche alle denkbaren 56-Bit-Schlüssel durchprobierte. Auch das Public-Key-System lässt sich austesten, etwa durch Chiffrieren spezieller Texte mit dem offenen Schlüssel und Analyse der Ergebnisse.

[0009] Darüber hinaus benötigt jeder Beteiligte einen privaten Schlüssel, den er geheimhalten muss, was mit einem entsprechenden Merkaufwand verbunden ist.

[0010] Der Erfindung liegt daher das Problem zugrunde, ein Codierungsverfahren zur Verfügung zu stellen, dass eine höhere Sicherheit bietet sowie den Aufwand für die Codierung für die Beteiligten verringert.

[0011] Die Erfindung löst diese Aufgabe durch die Einschaltung einer dritten Partei C, die den von der Partei A an die Partei B übermittelten Daten oder auch direkt an die Partei C gerichteten Daten einen privaten Schlüssel zuordnet, aus dem wiederum ein komplementärer öffentlicher Schlüssel berechnet wird. Der öffentliche Schlüssel wird beispielsweise per Datennetz der Partei A zugestellt, die damit nun ihre an die Partei B oder an die Partei C gerichteten Botschaften codiert. Die Partei B selbst kann jedoch die Botschaft nicht decodieren, da sie keinen Zugriff auf den privaten Schlüssel hat. Die Partei B sendet nun die codierte Botschaft an die dritte Partei C, die die mit dem öffentlichen Schlüssel codierte Botschaft wieder entschlüsselt und die nunmehr entschlüsselte Botschaft an die Partei B zurücksendet. Durch die dritte Partei C ist die Partei B durch Ver- und Entschlüsselungsprozesse nicht belastet und sie kann doch sicher sein, dass sie tatsächlich mit der richtigen Partei A kommuniziert oder Geschäfte tätigt, da nur die von dieser Partei A ausgehenden Daten entschlüsselt werden können.

[0012] Insbesondere für Verkäufe auf elektronischem Weg wie zum Beispiel über das Internet ist diese Art der Verschlüsselung geeignet, um das erforderliche Vertrauen zwischen dem Käufer und dem Verkäufer herzustellen. So kann zum Beispiel sichergestellt werden, dass der Verkäufer es tatsächlich mit der Person oder Institution zu tun hat, die sich als Partei A ausgibt. Einem Missbrauch durch einen Dritten, der sich als Partei A ausgibt, um auf Kosten der Partei A Geschäfte zu tätigen, ist damit vorgebeugt. So kann beispielsweise bei der ersten Aktion die Partei A ihren Namen und ihre Kreditkartennummer angeben. Um die Sicherheit zu erhöhen, kann diese erste Aktion nicht über die Partei B ab-

gewickelt werden, sondern die Partei A tritt direkt mit der Partei C in Verbindung, die der Kreditkartennummer in Verbindung mit dem Namen des A einen privaten Schlüssel zuordnet, der wiederum einen öffentlichen Schlüssel generiert. Der öffentliche Schlüssel wird der Partei A zugestellt, die damit zukünfig ihre Kreditkartennummer verschlüsselt, so dass nur noch die verschlüsselte Kreditkartennummer über das Netz verschickt wird. Die Partei B, die diese verschlüsselte Kreditkartennummer erhält, entschlüsselt sie jedoch nun nicht, sondern leitet sie an die Partei C weiter. Die Partei C kennt den privaten Schlüssel zur Dechiffrierung der verschlüsselten Kreditkartennummer und sendet nach der Entschlüsselung die entschlüsselte Nummer an die Partei B, die nun sicher sein kann, es tatsächlich mit der Person A zu tun zu haben, da nur diese über den öffentlichen Schlüssel, der zu dem privaten Schlüssel korrespondiert, verfügt.

[0013] Um die Sicherheit zu erhöhen, kann jedoch zusätzlich nach jeder Transaktion der Partei A von der Partei C ein neuer privater Schlüssel zugeordnet werden, der dann einen öffentlichen Schlüssel generiert. Auch wenn ein ungebetener Lauscher den öffentlichen Schlüssel errät, so nutzt ihm dies für die nachfolgende Transaktion nichts, da dann bereits ein anderer öffentlicher Schlüssel für das Verschicken der Botschaft verwendet wird.

[0014] Eine Dechiffrierung von Nachrichten ist nur durch Manipulationen der Partei C möglich, so dass sichergestellt werden muss, dass es sich hier um eine absolut vertrauenswürdige Institution handelt. Dies ist jedoch eine politische und keine technische Frage.

[0015] Weitere Einzelheiten und Vorteile der Erfindung ergeben sich aus der nachfolgenden Beschreibung und der Zeichnung. In der Zeichnung zeigen die Figuren 1 und 2 eine schematische Darstellung eines Ausführungsbeispiels der Erfindung anhand von Transaktionen zwischen Kunden und Lieferanten:

Fig.1: schematische Darstellung der Verbindung zwischen einem Kunden und einem Schlüsseldienst;

Fig.2: schematische Darstellung der Verbindung zwischen einem Kunden und einem Lieferanten.

[0016] Das in den Fig. 1 und 2 schematisch dargestellte Ausführungsbeispiel veranschaulicht, wie die Erfindung insbesondere für Verkäufe auf elektronischem Weg wie zum Beispiel über das Internet genutzt werden kann, um das erforderliche Vertrauen zwischen dem Käufer und dem Verkäufer sicherzustellen. Zu Beginn einer Transaktion zwischen Kunden und Lieferanten, wendet sich zweckmässigerweise ein potentieller Kunde K1 (Partei A) an einen Schlüsseldienst SD (Partei C) und meldet sich dort mit seinem Namen an. Es ist darüber hinaus vorteilhafterweise möglich, dass die potentiellen Lieferanten (Partei B) nur über den Schlüsseldienst erreichbar sind, so dass eine direkte Kontaktaufnahme zwischen den Kunden K und den Lieferanten L nicht möglich ist. Damit der Kunde K1 erfährt, mit welchen Lieferanten L er über den Schlüsseldienst SD in Kontakt treten kann, ist es insbesondere zweckmässig, dass der Kunde K1 zunächst völlig unverbindlich ohne Nennung seines Namens sich über das Angebot des Schlüsseldienstes SD informieren kann. Allerdings ist es im Rahmen der Erfindung auch denkbar, dass der Kunde K1 zunächst an den Lieferanten L1 herantritt und dieser ihn auf den Schlüsseldienst SD verweist und ihm erläutert, dass nur unter Einbeziehung des Schlüsseldienstes SD es möglich ist, mit ihm, dem Lieferanten L1, ein Geschäft zu tätigen.

[0017] Nach der Meldung des Namens von K1 sucht der Schlüsseldienst SD in seiner internen Datenbank, ob ihm dieser Name bereits bekannt ist. Ist dies nicht der Fall, so kreiert der Schlüsseldienst SD vorteilhafterweise zunächst einen Identifikationscode IC, den er dem K1 zweckmässigerweise nicht auf elektronischem Weg, sondern per Post zustellt, und trägt darüber hinaus K1 mit dem Identifikationscode in seine Datenbank ein. Insbesondere kann vorgesehen sein, dass vor der Eintragung des K1 in die Kundendatei der Schlüsseldienst sich nochmals von K1 bestätigen lässt, dass der Eintrag tatsächlich gewünscht ist, um keine unnötigen Eintragungen vorzunehmen.

[0018] Den Identifikationscode IC nutzt K1 nun bei der nächsten Transaktion mit dem Schlüsseldienst, indem er SD den Identifikationscode unverschüsselt übersendet. Zweckmässigerweise erfolgt erst nach dieser zweiten Transaktion die endgültige Eintragung des Kunden K1 in die Kundendatenbank von SD. Durch die zusätzliche Verwendung eines Identifikationscodes, der nur einmal für die endgültige Eintragung des K1 in die Kundendatei verwendet und nicht elekronisch zugestellt wird, erhöht sich die Sicherheit, da K1 nun nicht mit seinem direkten Namen etc. in Verbindung mit dem Schlüsseldienst SD tritt, sondern bereits unter einem Codenamen.

[0019] Der Schlüsseldienst SD kreiert nun für K1 einen privaten Schlüssel und berechnet daraus einen öffentlichen Schlüssel, den der Schlüsseldienst SD dem K1 auf elektronischem Weg zustellt. Um die Sicherheit zu erhöhen, kann jedoch vorteilhafterweise bei jeder Transaktion des K1 mit dem Schlüsseldienst SD oder einem Lieferanten L1 der Schlüsseldienst SD einen neuen privaten Schlüssel und dann daraus einen neuen öffentlichen Schlüssel für den Kunden K1 generieren. Auch wenn ein ungebetener Lauscher den öffentlichen Schlüssel errät, so nutzt ihm dies für die nachfolgende Transaktion nichts, da dann bereits ein anderer öffentlicher Schlüssel verwendet wird.

[0020] Neben seinem Namen und seiner Adresse kann der Kunde K1 beispielsweise auch seine Kreditkartennummer, seinen persönlichen Fingerabdruck oder das Muster seiner Iris mit dem öffentlichen Schlüssel verschlüsseln und über das Netz dem Schlüssel-

dienst SD schicken, der die Daten mit dem privaten Schlüssel entschlüsselt und diese Daten in der Datenbank ablegt.

[0021] Nachdem nunmehr der Schlüsseldienst alle wichtigen Daten des Kunden K1, die insbesondere für die zu tätigenden Geschäfte zwischen dem Kunden K1 und einem oder mehreren Lieferanten L1-Ln erforderlich sind, gespeichet hat, eröffnet der Schlüsseldienst SD dem Kunden K1 den Zugang zu allen Lieferanten, mit dem der Schlüsseldienst zusammenarbeitet.

[0022] Dabei ist es denkbar, dass alle Geschäfte nur über den Schlüsseldienst SD abgewickelt werden, so dass der Kunde K1 seinen Wunsch, mit welchem Lieferanten L1 er zusammenarbeiten will, dem SD verschlüsselt mitteilt, der ihn entschlüsselt und daraufhin die Verbindung zwischen dem K1 und einem Lieferanten L1 herstellt.

[0023] Die gleiche Verschlüsselungstechnik, die für die Kunden verwendet worden ist, kann dabei auch für die Lieferanten gelten, wobei auch dem L1 jeweils ein privater und ein öffentlicher Schlüssel zugeordnet wird. Auch hier wird der private Schlüssel beim Schlüsseldienst SD abgelegt, während der öffentliche Schlüssel dem L1 zugestellt wird.

[0024] Es ist jedoch auch möglich, dass die Geschäfte direkt zwischen K1 und L1 abgewickelt werden, wobei L1 sich bei jeder Transaktion beim Schlüsseldienst vergewissert, ob es sich tatsächlich um den Kunden K1 handelt, als der sich die mit L1 in Verbindung getretene Person/Institut ausgibt. Nur wenn die wahre Identität des Kunden K1 geklärt ist, kann das geplante Geschäft abgewickelt werden. Einem Missbrauch durch einen Dritten, der sich als Kunde K1 ausgibt, um auf Kosten des K1 Geschäfte zu tätigen, ist damit vorgebeugt. So kann beispielsweise bei der ersten Aktion der Kunde K1 seinen Namen und seine Kreditkartennummer angeben. Um die Sicherheit zu erhöhen, wird zweckmässigerweise wie bereits ausgeführt diese erste Aktion nicht über den Lieferanten L1 abgewickelt, sondern der Kunde K1 tritt direkt mit dem Schlüsseldienst SD in Verbindung, der der Kreditkartennummer in Verbindung mit dem Namen des A einen privaten Schlüssel zuordnet, der wiederum einen öffentlichen Schlüssel generiert. Der öffentliche Schlüssel wird dem Kunden K1 zugestellt, der damit zukünfig die Kreditkartennummer verschlüsselt, so dass nur noch die verschlüsselte Kreditkartennummer über das Netz verschickt wird. Der Lieferant L1, der diese verschlüsselte Kreditkartennummer erhält, entschlüsselt sie jedoch nun nicht, sondern leitet sie an den Schlüsseldienst SD weiter. SD kennt den privaten Schlüssel zur Dechiffrierung der verschlüsselten Kreditkartennummer und sendet nach der Entschlüsselung die entschlüsselte Nummer an den Lieferanten L1, der nun sicher sein kann, es tatsächlich mit dem Kunden K1 zu tun zu haben, da nur dieser über den öffentlichen Schlüssel, der zu dem privaten Schlüssel korrespondiert, verfügt.

[0025] Eine Dechiffrierung von Nachrichten ist nur durch Manipulationen des Schlüsseldienstes SD möglich, so dass sichergestellt werden muss, dass es sich hier um eine absolut vertrauenswürdige Institution handelt. Dies ist jedoch eine politische und keine technische Frage.

[0026] Die Erfindung ermöglicht somit durch die Einbeziehung einer Dritten Partei die Übermittlung von Daten sicherer zu gestalten und insbesondere die Sicherheit von elektronisch abgewickelten Verkaufstransaktionen zu erhöhen.

Patentansprüche

1. Verfahren zur Codierung von Daten D und Informationen, die auf elektronischem Weg über Datenübertragunsmittel von einer Partei A an eine Partei B übermittelt werden, **dadurch gekennzeichnet**, dass die Partei A an die Partei B und/oder an eine Partei C einen Datensatz D zunächst unverschlüsselt und/oder mit einem Code versehen übermittelt, wobei die Partei B die Daten D an die dritte Partei C weiterleitet, und die Partei C den Daten D einen privaten Schlüssel X zuordnet, der nur der Partei C bekannt ist, und aus diesem privaten Schlüssel X über einen in einer Richtung eineindeutigen Algorithmus einen öffentlichen Schlüssel Y generiert, der der Partei A zugestellt wird und der bei der folgenden Übermittlung von Daten D durch die Partei A an die Partei B und/oder an die Partei C zur Verschlüsselung der Daten D verwendet wird, wobei die Partei B wiederum die verschlüsselten Daten Y (D) an die Partei C schickt, und die Partei C mit Hilfe des den Daten Y(D) zugeordneten privaten Schlüssels X die Daten Y(D) entschlüsselt und die entschlüsselten Daten D an die Partei B sendet.

2. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass es sich bei der Partei A um einen Kunden, bei der Partei B um einen Lieferanten und bei der Partei C um einen Schlüsseldienst oder dergleichen handelt, der von einer Institution oder Organisation betrieben wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass es sich bei den Daten D um ein die Partei A charakterisierendes Merkmal handelt.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass es sich bei den Daten D um den Namen und/oder die Adresse der Partei A handelt.

5. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass es sich bei der Daten D um ein allgemeines Password, einen Fingerabdruck oder die Abbildung der Iris des Auges handelt, die der Partei A zugeordnet werden können.

6. Verfahren nach einem oder mehreren der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass nach jeder Übermittlung der Daten Y(D) von der Partei A an die Partei B und/oder an die Partei C der den Daten Y(D) zugeordnete private Schlüssel X von der Partei C geändert wird, ein entsprechend neuer öffentlicher Schlüssel Y2 generiert wird und dieser der Partei A für die nächste Übermittlung der Daten D mitgeteilt wird, so dass bei der nächsten Übermittlung die Daten D mit dem neuen öffentlichen Schlüssel Y2 verschlüsselt werden und als Daten Y2(D) verschickt werden, von der Partei C mit dem privaten Schlüssel X2 decodiert werden und dann die entschlüsselten Daten D an die Partei B zugestellt werden.

7. Verfahren nach einem oder mehreren der Ansprüche 1, dadurch gekennzeichnet, dass bei der Übermittlung von Daten D von der Partei B an die Partei A gleichfalls die Partei B die Daten D zunächst unverschlüsselt und/oder mit einem Code versehen an die Partei A und/oder an die Partei C übermittelt, wobei die Partei A die Daten D an die dritte Partei C weiterleitet, und die Partei C den Daten D einen privaten Schlüssel X zuordnet, der nur der Partei C bekannt ist, und aus diesem privaten Schlüssel X über einen in einer Richtung eineindeutigen Algorithmus einen öffentlichen Schlüssel Y generiert, der der Partei B zustellt wird und der bei der folgenden Übermittlung von Daten D durch die Partei B an die Partei A und/oder an die Partei C zur Verschlüsselung der Daten D verwendet wird, wobei die Partei A nunmehr die verschlüsselten Daten Y (D) wiederum an die Partei C schickt, und die Partei C mit Hilfe des den Daten Y(D) zugeordneten privaten Schlüssels X die Daten Y(D) entschlüsselt und die entschlüsselten Daten D an die Partei A sendet.

8. Verfahren nach einem oder mehreren der Ansprüche 1-7, dadurch gekennzeichnet, dass nach der ersten Kontaktaufnahme der Partei A mit der Partei B und/oder mit der Partei C eine erste Codierung von der Partei C an die Partei A auf nichtelektronischem Weg zugesendet wird, und dass die Partei A die Codierung bei ihrer zweiten Kontaktaufnahme mit der Partei B und/oder mit der Partei C verwendet.

9. Verfahren nach einem oder mehreren der Ansprüche 1-8, dadurch gekennzeichnet, dass die Partei A und/oder die Partei B und/oder die Partei C mehrere Personen, Institutionen oder Organisationen sein können.

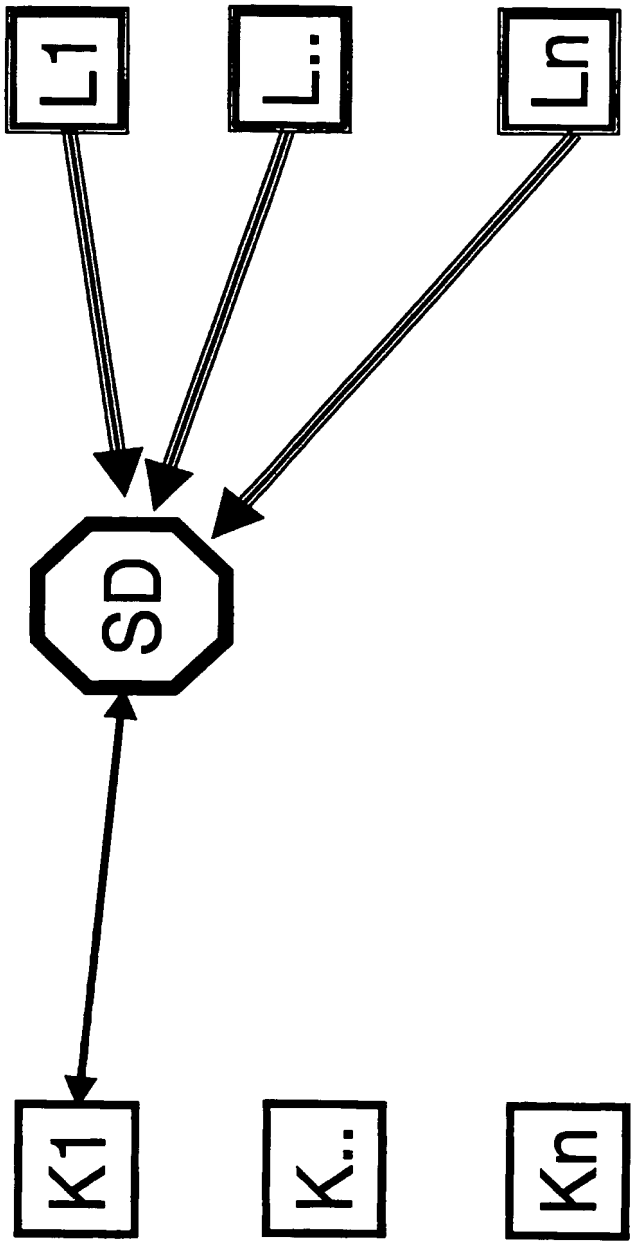

Fig. 1 ITC&C-1-Pat

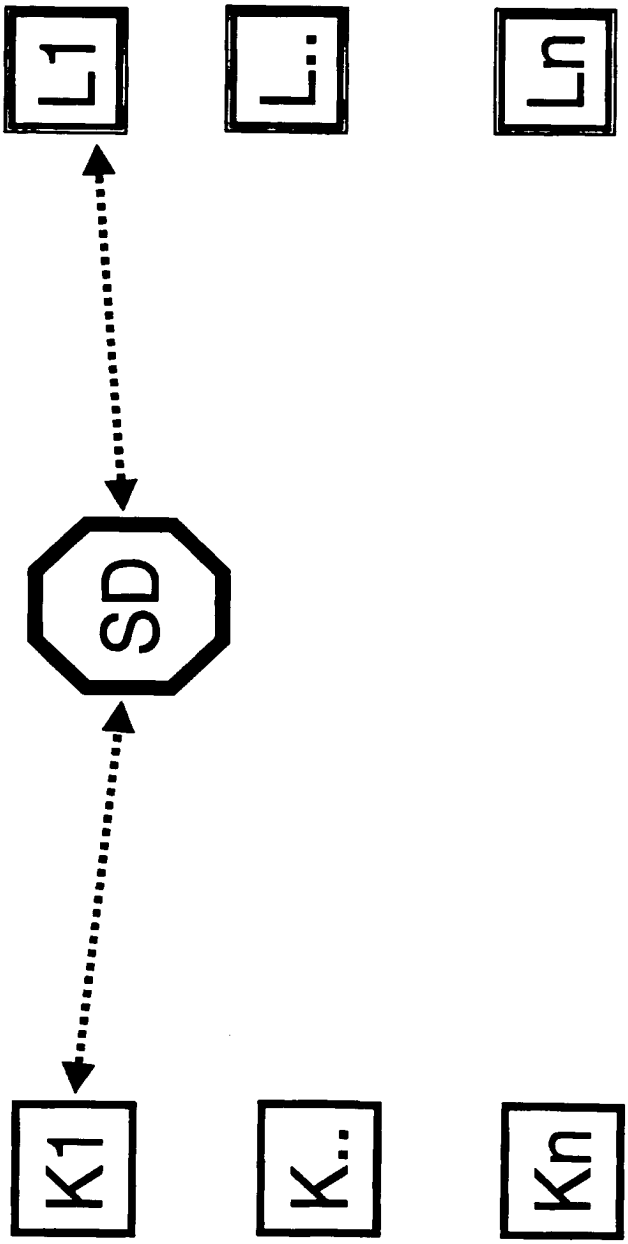

Fig. 2

ITC&C-1-Pat

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 99 10 8960

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.7)
A	MAMBO M ET AL: "PROXY CRYPTOSYSTEMS: DELEGATION OF THE POWER TO DECRYPT CIPHERTEXTS" IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, Bd. E80-A, Nr. 1, 1. Januar 1997 (1997-01-01), Seiten 54-63, XP000742245 ISSN: 0916-8508 * Zusammenfassung * * Seite 54, rechte Spalte, Zeile 5 - Zeile 22 * * Seite 59, linke Spalte, letzter Absatz - rechte Spalte, Zeile 16 *	1	H04L9/30 G07F7/10
A	EP 0 797 329 A (ALSTHOM CGE ALCATEL) 24. September 1997 (1997-09-24) * Spalte 1, Zeile 40 - Zeile 48 * * Spalte 2, Zeile 26 - Zeile 51 * * Spalte 4, Zeile 12 - Zeile 36 *	1	
			RECHERCHIERTE SACHGEBIETE (Int.Cl.7) H04L G07F

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	27. Oktober 1999	Holper, G

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C09)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 99 10 8960

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

27-10-1999

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0797329 A	24-09-1997	FR 2746566 A	26-09-1997
		CA 2200624 A	21-09-1997
		JP 10013401 A	16-01-1998
		NO 971263 A	22-09-1997
		US 5956406 A	21-09-1999

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82